Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

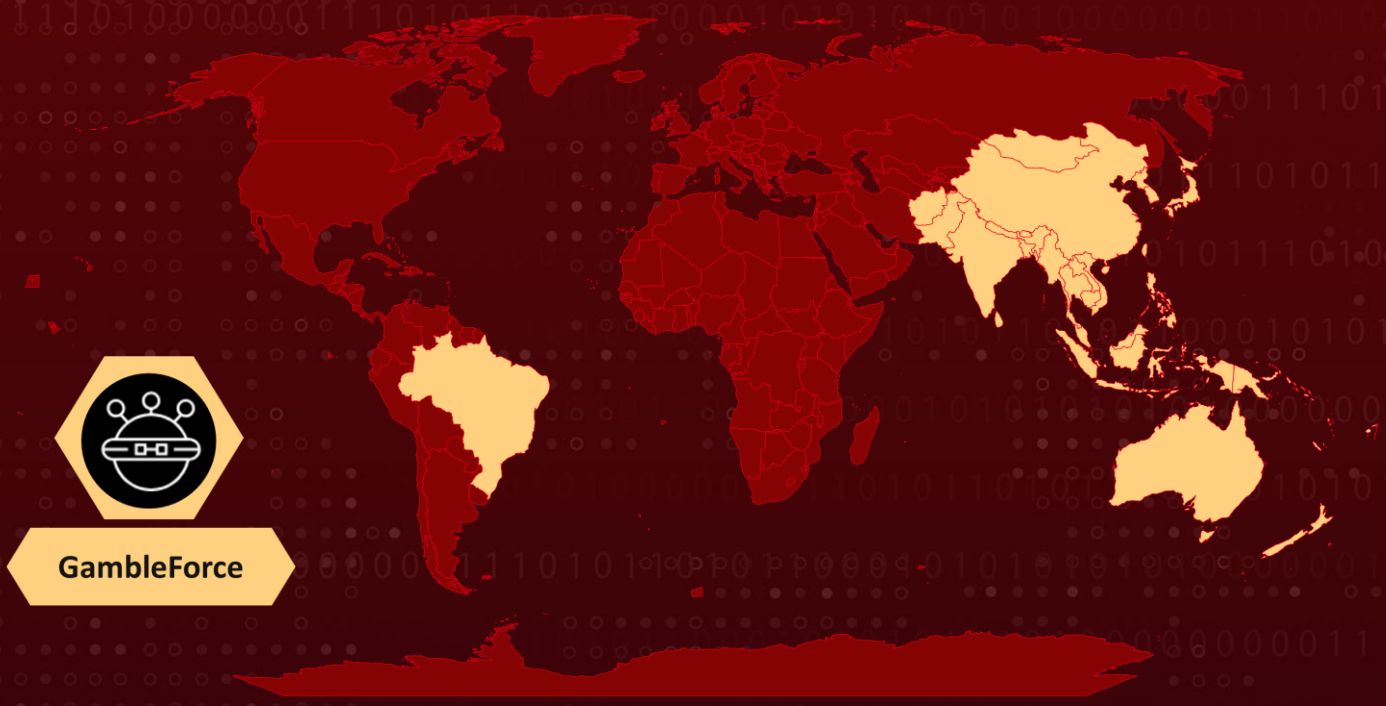
Unveiling GambleForce: A SQL Injection Gang

Date of Publication	Admiralty code	TA Number
December 15, 2023	A1	TA2023506

Summary

First Appearance: September 2023
Actor Name: GambleForce (aka EagleStrike)
Target Industries: Government, Gambling, Retail, and Travel
Target Region: Australia, Brazil, China, India, Indonesia, the Philippines, South Korea, Thailand and APAC region

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-23752	Joomla Improper Access Control Vulnerability	Joomla!	✗	✗	✓

Actor Details

#1 A novel threat actor known as GambleForce has been associated with a string of SQL injection attacks primarily directed at companies in the Asia-Pacific region. GambleForce employs a blend of basic yet remarkably effective techniques, incorporating SQL injections and exploiting vulnerabilities within website content management systems (CMS). These methods are utilized with the intent of unlawfully obtaining sensitive information, notably user credentials.

#2 GambleForce employed tools such as dirsearch, sqlmap, tinyproxy, and redis-rogue-getshell, utilizing them without any distinctive modifications and maintaining nearly all default settings. Notably, the version of Cobalt Strike identified on the gang's server was configured with commands in Chinese.

#3 GambleForce employs Cobalt Strike with malleable profiles, command and control (C&C) domains, and self-signed SSL certificates for both the teamserver and listeners. Notably, these certificates mimic the "Microsec e-Szigno Root CA" and "Cloudflare," deviating from default settings to enhance stealth and obfuscation.

#4 SQL injections are deployed in attacks utilizing sqlmap, an open-source penetration testing tool, to pinpoint vulnerable database servers. The attackers inject malicious SQL code into a publicly accessible web page, circumventing authentication protections and acquiring unauthorized access to sensitive data. As of now, GambleForce's motives and the specific use of the pilfered information remain undisclosed.

#5 In a Brazilian attack, GambleForce exploited CVE-2023-23752, a vulnerability within the Joomla CMS; however, this incident did not lead to the exfiltration of data. SQL attacks are prevalent due to companies' insecure input security, data validation, outdated software, and inappropriate database settings. This creates an ideal environment for SQL injection attacks on public-facing web applications. Proactive monitoring of systems is crucial, as intrusions can remain undetected for extended periods.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
GambleForce	Unknown **MOTIVE** Information theft and espionage	Australia, Brazil, China, India, Indonesia, the Philippines, South Korea, and Thailand	Government, Gambling, Retail, and Travel

Recommendations

Monitoring and Logging: Implement comprehensive logging of SQL errors and monitor the logs for suspicious activities. Set up alerts for unusual or potentially malicious database queries.

Least Privilege Principle: Limit the database user's permissions to the minimum necessary for the application to function. Avoid using accounts with unnecessary privileges. Avoid using the root/administrator account for normal application operations.

Web Application Firewalls (WAF): Implement a Web Application Firewall that can detect and block SQL injection attempts. WAFs can be configured to filter and block malicious traffic before it reaches your application.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0011 Command and Control
TA0010 Exfiltration	T1595 Active Scanning	T1595.002 Vulnerability Scanning	T1595.003 Wordlist Scanning
T1592 Gather Victim Host Information	T1592.002 Software	T1583 Acquire Infrastructure	T1583.001 Domains
T1583.004 Server	T1190 Exploit Public-Facing Application	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	Dns-supports[.]online, Windows.updates[.]wiki
IP	212.60.5[.]129, 38.54.40[.]156

Patch Details

Upgrade to version 4.2.8 or later

Link: https://downloads.joomla.org/

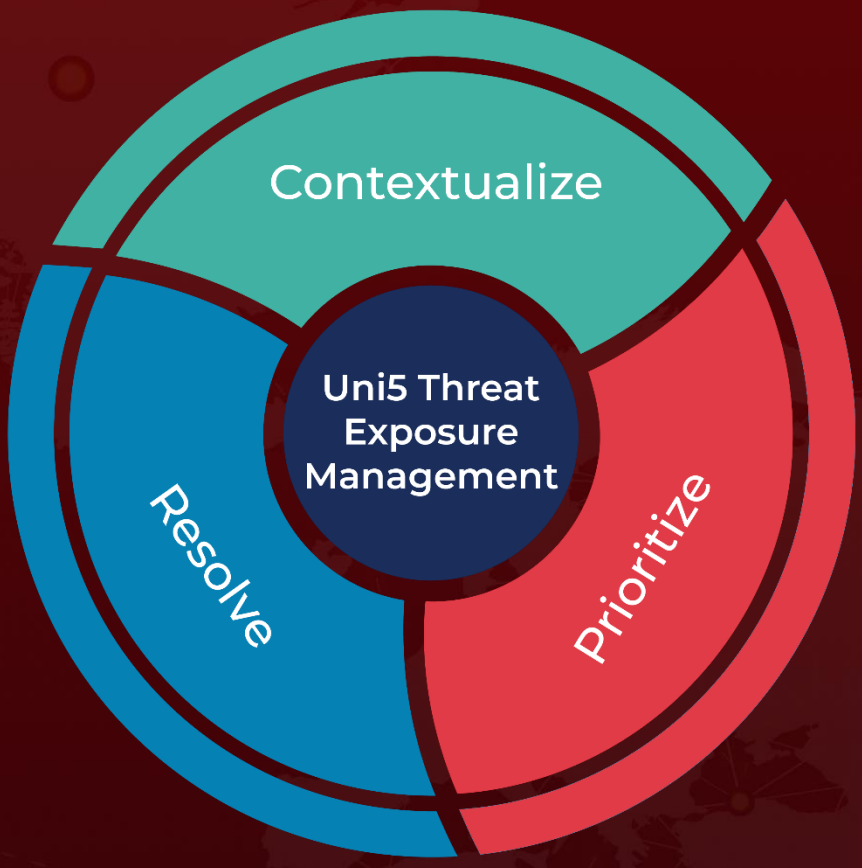
References

https://www.group-ib.com/blog/gambleforce-gang/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 15, 2023 • 5:15 AM

© 2023 All Rights are Reserved by Hive Pro®

More at www.hivepro.com